JOURNAL OF NUMBER THEORY 30, 243–266 (1988)

Witt Groups of Algebraic Integers

PARVATI SHASTRI*

School of Mathematics,
Tata Institute of Fundamental Research,
Bombay 400 005, India

Communicated by H. Zassenhaus

Received December 31, 1986; revised December 1, 1987

INTRODUCTION

For any commutative ring R, let WR denote the Witt group of non-singular symmetric bilinear forms over R. If F is an algebraic number field and D its ring of integers, we have an exact sequence (cf. [8, 93–94, 3.3, 3.4])

$$0 \to WD \to WF \to \bigsqcup_{\substack{0 \neq \mathfrak{p} \\ \mathfrak{p} \in \operatorname{spec} D}} W\bar{F}_{\mathfrak{p}} \to H(F)/H(F)^2 \to 0, \qquad \text{(A)}$$

where $\bar{F}_{\mathfrak{p}}$ denotes the residue class field of the completion $F_{\mathfrak{p}}$ of F with respect to the valuation induced by the prime ideal $\mathfrak{p}$ and $H(F)$ denotes the ideal class group of F. J. Milnor in [8] shows that WD is a finitely generated abelian group of rank r, where r is the number of real completions of F, and computes the order of the torsion subgroup of WD. In the special case $F = \mathbb{Q}$, $D = \mathbb{Z}$, he also shows that the sequence

$$0 \to W\mathbb{Z} \to W\mathbb{Q} \to \bigsqcup_{p} W(\mathbb{Z}/p\mathbb{Z}) \to 0, \qquad \text{(B)}$$

is indeed split. It is natural to ask, in general, for the structure of WD in terms of the arithmetical invariants of F and to determine conditions under which the inclusion $WD \subsetneq WF$ splits. This would give an explicit description of WF, as against the description (A), which is only up to extensions. In this paper, we deal with the above two questions for any number field and give a complete solution for the case of quadratic fields.

One may be led, in view of (B), to the naive belief that the sequence (A) is split for Euclidean number fields. However, in Section 4 we give some

* Author is presently a Visiting Member at the Tata Institute, Bombay.

0022-314X/88 $3.00

examples of Euclidean quadratic fields for which the sequence (A) does not split.

Here is a brief description of the contents of the paper: Section 1 contains a review of some basic results on quadratic forms over number fields, which we need in the later sections. In Sections 2 and 3 we compute the structure of WD and discuss conditions for the splitting of $WD \subsetneq WF$, in terms of certain invariants related to the unit group, the ideal class group, and the number of archimedean and dyadic completions of F (cf. 3.1–3.7). In Section 4, we compute the structure of WD for quadratic fields F and give necessary and sufficient conditions for the splitting of $WD \subsetneq WF$ purely in terms of the discriminant. In fact, for imaginary quadratic fields, we show that $WD \subsetneq WF$ always splits. In the final section, we compute the Witt group WD for certain cubic fields.

Notation. We fix the following notation for the rest of the paper.

WR: the Witt ring of nonsingular symmetric bilinear forms over any commutative ring R.

K^*: the group of nonzero elements of any field K.

For any algebraic number field F, we denote by

D_F: the ring of integers of F.

F^+: the group of totally positive elements of F.

U_F: the group of units of F.

U_F^+: the group of totally positive units of F.

F_v: the completion of F with respect to any valuation v of F.

$F_\mathfrak{p}$: the completion of F with respect to the valuation $v = v_\mathfrak{p}$ induced by the nonzero prime ideal $\mathfrak{p}$ of F.

r: the number of real completions of F.

c: the number of pairs of complex completions of F.

d: the number of dyadic completions of F.

Let L be a field of characteristic $\neq 2$. The notion of quadratic forms over L and symmetric bilinear forms over L coincide and by a *form* over L, we mean a quadratic form over L whose associated bilinear form is nonsingular. To simplify notation, we shall denote by q the class in the Witt ring of the form q. For forms q, q', we write $q = q'$ to mean that their classes in the Witt ring are the same, whereas $q \simeq q'$ means that q and q' are isometric. We denote by IL the fundamental ideal of WL consisting of even dimensional forms over L and by I^nL the nth power of IL for $n \geqslant 2$. For a form q over L we denote by $\mathfrak{d}(q)$ the (signed) discriminant of q.

We cite [11] as reference for all basic facts on quadratic forms and [10] for classical results on quadratic forms over number fields.

1. Some Basic Results on Quadratic Forms over Number Fields

We record in this section a few results on quadratic forms over number fields which will be used in the later sections. The proofs of these results can be found in [11].

THEOREM 1.1. *Let F be an algebraic number field. A quadratic form over F is determined (up to isometry) by its dimension, discriminant, Witt invariant, and signatures (cf.* [11, p. 224, 6.6]).

THEOREM 1.2 (Elman and Lam). *Let K be any field. Then the following conditions are equivalent:*

(i) *Quadratic forms over K are determined (up to isometry) by dimension, discriminant, Witt invariant, and signatures.*

(ii) *The ideal I^3K of WK is torsion free (cf.* [11, p. 91, 14.6]).

THEOREM 1.3 (Pfister's Local–Global Principle). *Let F be an algebraic number field with r real completions ($r \geqslant 0$) and let $\sigma: WF \to \bigsqcup_r W\mathbb{R}$ be the signature homomorphism, i.e., the homomorphism induced by the distinct real imbeddings $\sigma_i: F \to \mathbb{R}$, $1 \leqslant i \leqslant r$. Then* $\ker \sigma$ *is the torsion subgroup of WF (cf.* [11, p. 56, 7.3]).

Let W_tF denote the torsion subgroup of WF. Then by the above theorem $W_tF = \ker \sigma$. Let $\mathfrak{n}(WF)$ denote the nilradical of WF. Then in view of [8, pp. 68, 69, 3.6, 3.8], we have $\mathfrak{n}(WF) = W_tF$, if $r \geqslant 1$, and $\mathfrak{n}(WF) = IF$, if $r = 0$.

COROLLARY 1.4. *Let F be an algebraic number field. Then I^3F is torsion free and hence $I^3F \cap \mathfrak{n}(WF) = (0)$.*

Proof. Immediate from (1.1), (1.2), (1.3), and the remarks following (1.3).

PROPOSITION 1.5. *Let F be an algebraic number field. Then the exponent of $\mathfrak{n}(WF)$ divides* 4.

Proof. For $q \in \mathfrak{n}(WF)$, $4q = \langle 1, 1\rangle \otimes \langle 1, 1\rangle \otimes q$ belongs to I^3F. Thus $4q \in I^3F \cap \mathfrak{n}(WF) = (0)$ by (1.4).

Let K be any field. For $\alpha, \beta \in K^{\cdot}$, we define the symbol $S(\alpha, \beta)$ by

$$S(\alpha, \beta) = 1 \quad \text{if} \quad \langle 1, -\alpha, -\beta, \alpha\beta\rangle \text{ splits}$$

$$= -1 \quad \text{if} \quad \langle 1, -\alpha, -\beta, \alpha\beta\rangle \text{ does not split.}$$

For an n-dimensional quadratic form $\langle a_1, ..., a_n \rangle$ over K, we define

$$S\langle a_1, ..., a_n \rangle = \prod_{i<j} S(a_i, a_j).$$

We sometimes write S_K instead of S to stress the field in question. For a v-adic completion of a number field F, we shall abbreviate $S_{F_v} = S_v$.

THEOREM 1.6. (*Hilbert Reciprocity*). *Let F be an algebraic number field. For any valuation v of F let an n-dimensional form ψ_v over F_v be given. Then there exists a form ϕ over F with $\phi_v \simeq \psi_v$ for all v, if and only if the following conditions are satisfied*:

(i) *There exists $\mathfrak{d} \in F^*$ with $\operatorname{disc} \psi_v =$ class of $\mathfrak{d}$ in F_v^*/F_v^{*2} for all v;*

(ii) *the number of v for which $S_v(\psi_v) = -1$ is finite and even, i.e., $\prod_v S_v(\psi_v) = 1$ (cf.* [11, p. 225, 6.10]).

PROPOSITION 1.7. *Let F be an algebraic number field. Then any element of $\mathfrak{n}(WF)$ is represented by a form of dimension 2 or 4.*

Proof. If ω is in $\mathfrak{n}(WF)$, then ω is hyperbolic over all archimedean completions. If $\dim \omega > 4$, then ω is isotropic over all nonarchimedean completions, since every form of dimension $\geqslant 5$ is isotropic over a p-adic field (cf. [11, p. 217, 4.2]). Thus if $\omega \in \mathfrak{n}(WF)$ and $\dim \omega > 4$, it is isotropic over F by the Hasse–Minkowski theorem. Hence ω is represented by a form of dimension $\leqslant 4$. Further, since $\mathfrak{n}(WF) \subset IF$, it follows that it is represented by a form of dimension 2 or 4.

PROPOSITION 1.8. *Let F be an algebraic number field. Then every form in $\mathfrak{n}(WF)$ of dimension 4 is universal.*

Proof. Let $\lambda \in F^*$ and $\omega \in \mathfrak{n}(WF)$ be a form of dimension 4. Since $\mathfrak{n}(WF) \subset \ker \sigma$, ω is hyperbolic over all archimedean completions of F. Since any form of dimension $\geqslant 5$ is isotropic over all p-adic completions, $\omega \perp \langle -\lambda \rangle$ is isotropic over all completions of F. Hence by the Hasse–Minkowski theorem $\omega \perp \langle -\lambda \rangle$ is isotropic over F. This proves the proposition.

PROPOSITION 1.9. *Let K be any field and let $\lambda \in K^*$. Suppose $\langle 1, a, b, ab \rangle$ represents λ. Then $\langle 1, a, b, ab \rangle \simeq \lambda \langle 1, a, b, ab \rangle$.*

Proof. See [11 p. 69, 10.1, 10.4].

COROLLARY 1.10. *If $\omega = 2\langle a, b \rangle$ is in $\mathfrak{n}(WF)$, then $\omega = 2\langle 1, ab \rangle$.*

Proof. We have, $\omega = 2\langle a, b\rangle = \langle a, b, a, b\rangle = a\langle 1, ab, 1, ab\rangle = 2\langle 1, ab\rangle$ by (1.8) and (1.9).

For any prime ideal $\mathfrak{p}$, let $\bar{F}_\mathfrak{p}$ denote the residue class field at $\mathfrak{p}$ of the number field F. We have an additive homomorphism $\partial_\mathfrak{p}: WF \to W\bar{F}_\mathfrak{p}$ defined as follows: If $\pi_\mathfrak{p}$ is a parameter at $\mathfrak{p}$, any form q over F can be written as $\langle b_1, ..., b_n\rangle \pi_\mathfrak{p} \perp \langle c_1, ..., c_k\rangle$ over $F_\mathfrak{p}$, with b_i, c_j local units for $\mathfrak{p}$. We define $\partial_\mathfrak{p}(q) = \langle \bar{b}_1, ..., \bar{b}_n\rangle$, $\bar{b}_i$ denoting the image of b_i in $\bar{F}_\mathfrak{p}$. We denote by ∂ the additive homomorphism $\bigsqcup_\mathfrak{p} \partial_\mathfrak{p}: WF \to \bigsqcup_\mathfrak{p} W\bar{F}_\mathfrak{p}$, induced by $\partial_\mathfrak{p}$ and we have an exact sequence (cf. [8, p. 93, 3.3])

$$0 \longrightarrow WD \xrightarrow{i} WF \xrightarrow{\partial} \bigsqcup_\mathfrak{p} W\bar{F}_\mathfrak{p}.$$

We shall identify WD with $\ker \partial$ through i.

We denote $\mathfrak{n}(WF) \cap WD$ by $\mathfrak{n}(WD)$. Thus, if $r \geqslant 1$, $\mathfrak{n}(WD) = \mathfrak{n}(WF) \cap WD = W_r F \cap WD$. If $r = 0$, $\mathfrak{n}(WD) = \mathfrak{n}(WF) \cap WD \subset IF$.

Let $H^*(F)$ denote the ideal class group of F in the *narrow sense*, i.e., the quotient of the free abelian group of all fractional ideals of F modulo the subgroup of all principal ideals of F generated by totally positive elements of F. We note that if F is totally imaginary (i.e., $r = 0$) then the ideal class group in the narrow sense is the same as the usual class group. We denote the 2-torsion subgroup of $H^*(F)$ by ${}_2H^*(F)$ and its order by 2^l.

THEOREM 1.11. *Let F be an algebraic number field and let σ be the total signature homomorphism $WF \to \bigsqcup_r W\mathbb{R}$. Then,*

(a) *$\sigma(WD)$ is a free abelian group of rank r.*

(b) *$\mathfrak{n}(WD)$ is a finite abelian group of order $2^{c+l+d-1}$ where c, d are as explained in the introduction and l is as defined above.*

(c) *If $r \geqslant 1$, $WD \cong \mathbb{Z}^r \oplus \mathfrak{n}(WD)$ and if $r = 0$, WD is a finite abelian group of order 2^{c+l+d}.*

Proof. See [8, pp. 95–99, 4.1–4.6].

2. THE STRUCTURE OF THE GROUP $\mathfrak{n}(WD)$ AS A SUBGROUP OF $\mathfrak{n}(WF)$

The group structure of WD and the splitting property of $WD \subsetneq WF$ are closely related to the structure of $\mathfrak{n}(WD)$ and the splitting property of $\mathfrak{n}(WD) \subsetneq \mathfrak{n}(WF)$. The aim of this section is to study the group $\mathfrak{n}(WD)$ and to give necessary and sufficient conditions for the splitting of $\mathfrak{n}(WD) \subsetneq \mathfrak{n}(WF)$.

THEOREM 2.1. *Let F be an algebraic number field and let $K = F(\sqrt{-1})$. Let $N: K^* \to F^*$ denote the norm homomorphism. Let $\mathscr{H}$ be the subgroup of $H^*(F)$ generated by ideal classes $\tilde{\mathfrak{a}}$ with $\mathfrak{a}^2 = (N(\mu))$ for some $\mu \in K^*$ ($\mathscr{H}$ is a subgroup of ${}_2H^*(F)$). We then have*

$$\mathfrak{n}(WD) \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^u,$$

where s, t, and u are determined by

$$2^s = |U_F^+/(N(K) \cap U_F^+)|,$$
$$2^t = |{}_2H^*(F)/\mathscr{H}|,$$

$2s + 2t + u = c + l + d - 1$; *$c$, d, l being as in Section* 1.

For the proof of the theorem we need some auxiliary results.

LEMMA 2.2. *Let G be a finite abelian group whose exponent divides* 4. *Then $|G|$ and $|2 \cdot G|$ determine the group G up to isomorphism. More precisely, if $|2 \cdot G| = 2^m$, then $G \simeq (\mathbb{Z}/4\mathbb{Z})^m \oplus (\mathbb{Z}/2\mathbb{Z})^n$ with $|G| = 2^{2m+n}$.*

Proof. Follows from the structure theorem for finite abelian groups.

COROLLARY 2.3. $\mathfrak{n}(WD) \simeq (\mathbb{Z}/4\mathbb{Z})^m \oplus (\mathbb{Z}/2\mathbb{Z})^n$, *where* $|2 \cdot \mathfrak{n}(WD)| = 2^m$ *and* $2m + n = c + l + d - 1$.

Proof. Follows from (1.11) and the above lemma.

PROPOSITION 2.4. (i) *Let q be an element of WD. Then, the ideal generated by $\mathfrak{d}(q)$ is the square of some fractional ideal of F.*

(ii) *For any $\lambda \in F^*$, $\langle \lambda \rangle$ is in WD if and only if $(\lambda) = \mathfrak{a}^2$ for some fractional ideal $\mathfrak{a}$ of F.*

(iii) *For $\lambda \in F^*$, $\langle 1, -\lambda \rangle \in \mathfrak{n}(WD)$ if and only if $\lambda \in F^+$ and $(\lambda) = \mathfrak{a}^2$ for some fractional ideal $\mathfrak{a}$ of F.*

Proof. (i) Since $q \in WD$, we have, $\partial_{\mathfrak{p}}(q) = 0$ for all nonzero prime ideals $\mathfrak{p}$ of D. If $q \simeq q_1 \perp \pi q_2$ over $F_{\mathfrak{p}}$ with q_1, q_2 unimodular, and π denoting a parameter at $\mathfrak{p}$, then $\partial_{\mathfrak{p}}(q) = \bar{q}_2 = 0$ implies that the dimension of q_2 is even; i.e., the ideal generated by $\mathfrak{d}(q)$ is divisible by an even power of $\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p}$ of F. Hence the ideal generated by $\mathfrak{d}(q)$ is the square of some ideal $\mathfrak{a}$ of F.

(ii) If $\langle \lambda \rangle \in WD$, then $(\lambda) = \mathfrak{a}^2$ by (i). Conversely, if $(\lambda) = \mathfrak{a}^2$, then by the definition of ∂, $\partial_{\mathfrak{p}}(\langle \lambda \rangle) = 0$, for all $\mathfrak{p}$; i.e., $\partial(\langle \lambda \rangle) = 0$. This implies that $\langle \lambda \rangle \in \ker \partial = WD$.

(iii) Let $\langle 1, -\lambda\rangle \in \mathfrak{n}(WD)$. Then, $\langle 1, -\lambda\rangle$ is hyperbolic over all the real completions. Hence $\lambda \in F^+$ and $(\lambda) = \mathfrak{a}^2$ by (i). Conversely, suppose $\lambda \in F^+$ and $(\lambda) = \mathfrak{a}^2$. Then, $\langle 1, -\lambda\rangle \in \mathfrak{n}(WF) \cap WD = \mathfrak{n}(WD)$.

Let $\mathscr{D}$ denote the set of all $\lambda \in F^+$ which occur as discriminants of forms belonging to WD. Clearly $\mathscr{D} = \{\lambda \in F^+/(\lambda) = \mathfrak{a}^2$ for some ideal $\mathfrak{a}$ of $F\}$ (cf. 2.4) and $F^{\cdot 2} \subset \mathscr{D}$.

PROPOSITION 2.5. (a) *The (signed) discriminant* $\mathfrak{d}$ *induces an isomorphism* $IF/I^2F \to^{\mathfrak{d}} F^{\cdot}/F^{\cdot 2}$ *whose inverse* $f: F^{\cdot}/F^{\cdot 2} \to IF/I^2F$ *is given by* $f(\bar{\lambda}) = \langle\overline{1, -\lambda}\rangle$.

(b) *The restriction of* $\mathfrak{d}$ *induces isomorphisms*

(i) $\mathfrak{d}: \mathfrak{n}(WF)/(\mathfrak{n}(WF) \cap I^2F) \xrightarrow{\sim} F^+/F^{\cdot 2}$,

(ii) $\mathfrak{d}: \mathfrak{n}(WD)/(\mathfrak{n}(WD) \cap I^2F) \xrightarrow{\sim} \mathscr{D}/F^{\cdot 2}$,

whose inverses are given by the restrictions of f *to* $F^+/F^{\cdot 2}$ *and to* $\mathscr{D}/F^{\cdot 2}$, *respectively.*

Proof. (a) See [11, p. 82, 12.10].

(b) $q \in \mathfrak{n}(WF)$ $(\subset \ker \sigma) \Leftrightarrow \mathfrak{d}(q)$ *is totally positive. Hence the image of* $\mathfrak{n}(WF)/(\mathfrak{n}(WF) \cap I^2F)$ *under* $\mathfrak{d}$ *is* $F^+/F^{\cdot 2}$. *Since* $IF/I^2F \xrightarrow{\sim} \{\langle 1, \lambda\rangle \mid \lambda \in F^{\cdot}\}$, *the image of* $\mathfrak{n}(WD)/(\mathfrak{n}(WD) \cap I^2F)$ *under* $\mathfrak{d}$ *is* $\mathscr{D}/F^{\cdot 2}$, *by* (2.4)(iii). *This proves* (b).

PROPOSITION 2.6. (a) *The correspondence* $\bar{\lambda} \to 2\langle 1, -\lambda\rangle$ *defines a surjective homomorphism* $F^+/F^{\cdot 2} \to^{\theta} 2 \cdot \mathfrak{n}(WF)$.

(b) *The restriction of the above homomorphism induces an isomorphism (which we denote by* θ *itself),* $\theta: \mathscr{D}/(N(K) \cap \mathscr{D}) \to 2 \cdot \mathfrak{n}(WD)$, *where* $K = F(\sqrt{-1})$ *and* $N: K^{\cdot} \to F^{\cdot}$ *is the norm homomorphism.*

Proof. (a) We have a surjective homomorphism, $\mathfrak{n}(WF) \to 2 \cdot \mathfrak{n}(WF)$ given by $q \to 2 \cdot q$. Since $2(\mathfrak{n}(WF) \cap I^2F) \subset \mathfrak{n}(WF) \cap I^3F = (0)$ (cf. (1.4)) this induces a surjective homomorphism $\mathfrak{n}(WF)/(\mathfrak{n}(WF) \cap I^2F) \to 2 \cdot \mathfrak{n}(WF)$. Composing this with the homomorphism $f: F^+/F^{\cdot 2} \to \mathfrak{n}(WF)/(\mathfrak{n}(WF) \cap I^2F)$ of (2.5) we get a surjective homomorphism $\theta: F^+/F^{\cdot 2} \to 2 \cdot \mathfrak{n}(WF)$. Clearly $\theta(\bar{\lambda}) = 2 \cdot f(\bar{\lambda}) = 2\langle 1, -\lambda\rangle$. This proves (a).

(b) Since the image of $\mathscr{D}/F^{\cdot 2}$ under f is $\mathfrak{n}(WD)/(\mathfrak{n}(WD) \cap I^2F)$ (cf. (2.5)), by restricting θ we get a surjective homomorphism $\mathscr{D}/F^{\cdot 2} \to^{\theta} 2 \cdot \mathfrak{n}(WD)$. We claim that $\ker \theta = N(K) \cap \mathscr{D}/F^{\cdot 2}$. For, if $\lambda \in \mathscr{D}$, $\theta(\bar{\lambda}) = 0 \Leftrightarrow 2\langle 1, -\lambda\rangle$ is hyperbolic $\Leftrightarrow \langle 1, 1, -\lambda\rangle$ is isotropic $\Leftrightarrow \lambda$ is a sum of two squares in $F \Leftrightarrow \lambda \in N(K)$. This proves the claim and (b) follows.

In the next proposition we determine the order of $\mathscr{D}/N(K) \cap \mathscr{D}$.

PROPOSITION 2.7. *The order of the group* $\mathscr{D}/N(K)\cap\mathscr{D}$ *is equal to* 2^{s+t} *where* 2^s *is the index of* $N(K)\cap U_F^+$ *in* U_F^+ *and* 2^t *is the index of* $\mathscr{H}$ *in* ${}_2H^*(F)$, $\mathscr{H}$ *being as in* (2.1).

Proof. We define $f:\mathscr{D}\to H^*(F)$ by $\lambda\mapsto\bar{\mathfrak{a}}$, if $\mathfrak{a}^2=(\lambda)$. Then f is a well-defined homomorphism of groups, whose image is precisely ${}_2H^*(F)$. This induces a surjective homomorphism,

$$f:\mathscr{D}/N(K)\cap\mathscr{D}\to {}_2H^*(F)/\mathscr{H}.$$

Let i denote the map $U_F^+\to\mathscr{D}/N(K)\cap\mathscr{D}$ induced by the inclusion $U_F^+\subsetneq\mathscr{D}$. Then we have a sequence

$$1\longrightarrow U_F^+/(N(K)\cap U_F^+)\to\mathscr{D}/N(K)\cap\mathscr{D}\xrightarrow{f}{}_2H^*(F)/\mathscr{H}\longrightarrow 1. \quad (*)$$

We claim this sequence is exact. In view of the above discussions, it is enough to prove $\ker f=i(U_F^+/N(K)\cap U_F^+)$. Clearly $i(U_F^+/N(K)\cap U_F^+)\subset\ker f$. Let $\bar{\lambda}\in\ker f$, with $\lambda\in\mathscr{D}$. Then $(\lambda)=(N(\mu))$ for some $\mu\in K$, so that $\lambda=u\cdot N(\mu)$ for some $u\in U_F$. Since λ and $N(\mu)$ are totally positive, u is totally positive. Hence $\bar{\lambda}=\bar{u}$ in $\mathscr{D}/N(K)\cap\mathscr{D}$ so that $\lambda\in i(U_F^+/N(K)\cap U_F^+)$. Thus $\ker f=i(U_F^+/N(K)\cap U_F^+)$. Hence $(*)$ is exact. Since all the groups in $(*)$ are finite, of 2-torsion, we have $|\mathscr{D}/N(K)\cap\mathscr{D}|=|U_F^+/N(K)\cap U_F^+|\cdot|{}_2H^*(F)/\mathscr{H}|=2^{s+t}$ where $|U_F^+/N(K)\cap U_F^+|=2^s$ and $|{}_2H^*(F)/\mathscr{H}|=2^t$.

COROLLARY 2.8. $|2\cdot\mathfrak{n}(WD)|=2^{s+t}$.

Proof. Immediate from (2.6) and (2.7).

Proof of Theorem 2.1. By (1.11), $|\mathfrak{n}(WD)|=2^{c+l+d-1}$. By (2.8), $|2\cdot\mathfrak{n}(WD)|=2^{s+t}$. Hence by (2.3), it follows that $\mathfrak{n}(WD)\supsetneq(\mathbb{Z}/4\mathbb{Z})^{s+t}\oplus(\mathbb{Z}/2\mathbb{Z})^u$ where $2s+2t+u=c+l+d-1$. Hence the theorem follows.

In the rest of this section we discuss the question of the splitting of $\mathfrak{n}(WD)\subsetneq\mathfrak{n}(WF)$. To begin with, we record the following fact from group theory, which will be needed for our discussions. We recall that a subgroup H of an abelian group G is called *pure* if $h\in H$, $h=ny$, n an integer, $y\in G$, imply $h=nh_1$ with $h_1\in H$.

THEOREM 2.9 [6, p. 18, Th. 7]. *Let* G *be an abelian group (not necessarily finitely generated) and let* H *be a subgroup of bounded exponent. Then* H *is a direct summand of* G *if and only if* H *is pure in* G.

THEOREM 2.10. *The subgroup* $\mathfrak{n}(WD)$ *is a direct summand of* $\mathfrak{n}(WF)$ *if and only if* $|2\cdot\mathfrak{n}(WD)|=|2\cdot\mathfrak{n}(WF)\cap\mathfrak{n}(WD)|$ *(i.e., if and only if an element of* $\mathfrak{n}(WD)$ *which is 2-divisible in* $\mathfrak{n}(WF)$ *is 2-divisible in* $\mathfrak{n}(WD)$*).*

Proof. By (1.5), the exponent of $\mathfrak{n}(WF)$ divides 4, so that $\mathfrak{n}(WD)$ is a subgroup of bounded exponent. By (2.9), $\mathfrak{n}(WD)$ is a direct summand of $\mathfrak{n}(WF)$ if and only if $\mathfrak{n}(WD)$ is a pure subgroup of $\mathfrak{n}(WF)$. Since the exponent of $\mathfrak{n}(WF)$ divides 4, $\mathfrak{n}(WD)$ is a pure subgroup of $\mathfrak{n}(WF)$ if and only if every element of $\mathfrak{n}(WD)$ which is 2-divisible in $\mathfrak{n}(WF)$ is 2-divisible in $\mathfrak{n}(WD)$. Since $\mathfrak{n}(WD)$ is a finite group, this is equivalent to the condition $|2\cdot\mathfrak{n}(WD)| = |2\cdot\mathfrak{n}(WF)\cap\mathfrak{n}(WD)|$. Hence the theorem follows.

In what follows, we determine the order of $2\cdot\mathfrak{n}(WF)\cap\mathfrak{n}(WD)$ in terms of the dyadic primes and give an upper bound for the order of $2\cdot\mathfrak{n}(WD)$.

PROPOSITION 2.11. *An element $\omega\in I^2F\cap\mathfrak{n}(WF)$ is 2-divisible in $\mathfrak{n}(WF)$ if and only if $S_\mathfrak{p}(\omega)=1$ for all $\mathfrak{p}$ for which -1 is a square in $F_\mathfrak{p}$ (where $S_\mathfrak{p}$ denotes the local symbol defined in Section 1).*

Proof. By (2.5)(b) $2\cdot\mathfrak{n}(WF)=\{2\langle 1,-\lambda\rangle/\lambda\in F^+/F^{\cdot 2}\}$. Since $2\langle 1,-\lambda\rangle$ is hyperbolic over $F_\mathfrak{p}$ for all $\mathfrak{p}$ for which -1 is a square in $F_\mathfrak{p}$, $S_\mathfrak{p}(\omega)=1$ for all such $\mathfrak{p}$ and for all $\omega\in 2\cdot\mathfrak{n}(WF)$. Conversely suppose $\omega\in I^2F\cap\mathfrak{n}(WF)$ and $S_\mathfrak{p}(\omega)=1$ for all $\mathfrak{p}$ for which -1 is a square in $F_\mathfrak{p}$. Let $\omega=\langle 1,a,b,ab\rangle$, $a,b\in F^\cdot$ (cf. (1.8), (1.9)). Let $\mathfrak{p}_1\cdots\mathfrak{p}_m$ be the primes such that $S_{\mathfrak{p}_i}(\omega)=-1$, $1\leqslant i\leqslant m$. By hypothesis -1 is not a square in $F_{\mathfrak{p}_i}$, $i=1,\ldots,m$, so that $\langle -1,a,b,ab\rangle$ has discriminant $-1\neq 1$ in $F^\cdot_{\mathfrak{p}_i}/F^{\cdot 2}_{\mathfrak{p}_i}$ for all $i=1,\ldots,m$. Hence $\langle -1,a,b,ab\rangle$ is isotropic over $F_{\mathfrak{p}_i}$ for $i=1,\ldots,m$. Therefore $\langle a,b,ab\rangle$ represents 1 over $F_{\mathfrak{p}_i}$ for $i=1,\ldots,m$. However, $\langle 1,a,b,ab\rangle$ is hyperbolic over all other completions. This implies that $\langle a,b,ab\rangle$ represents 1 over all completions. Hence by the Hasse–Minkowski theorem, $\langle a,b,ab\rangle$ represents 1 over F. Thus, $\omega=\langle 1,a,b,ab\rangle\simeq\langle 1,1,\lambda,\lambda\rangle$ for some $\lambda\in F^\cdot$. The condition $\omega\in I^2F\cap\mathfrak{n}(WF)$ implies that λ is totally negative so that $\langle 1,\lambda\rangle\in\mathfrak{n}(WF)$ and $\omega=2\langle 1,\lambda\rangle$; i.e., ω is 2-divisible in $\mathfrak{n}(WF)$. Hence the proposition follows.

PROPOSITION 2.12. *Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_m$ $(m\geqslant 0)$ be any finite set of prime ideals $(\neq(0))$ of F and let $J=\{\omega\in I^2F\cap\mathfrak{n}(WF)\mid S_\mathfrak{p}(\omega)=1$ for all $\mathfrak{p}\neq\mathfrak{p}_i$, $1\leqslant i\leqslant m\}$. Then $|J|=1$ if $m=0$ and $|J|=2^{m-1}$ if $m\geqslant 1$.*

Proof. J is a subgroup of $I^2F\cap\mathfrak{n}(WF)=I^2F\cap\ker\sigma$. We have a homomorphism $S: J\to(\mathbb{Z}/2\mathbb{Z})^m$ given by $S(\omega)=(S_{\mathfrak{p}_i}(\omega))_{1\leqslant i\leqslant m}$, $\omega\in J$. By the Hasse–Minkowski theorem S is injective. If $m=0$, this implies that $|J|=1$. Suppose $m\geqslant 1$. By (1.6) for any element ω of $I^2F\cap\mathfrak{n}(WF)$, $\prod S_\mathfrak{p}(\omega)=1$ and conversely given local symbols $(\varepsilon_\mathfrak{p})$ such that $\prod\varepsilon_\mathfrak{p}=1$ (where $\varepsilon_\mathfrak{p}=\pm 1$), there is an element ω of $I^2F\cap\mathfrak{n}(WF)$ such that $S_\mathfrak{p}(\omega)=\varepsilon_\mathfrak{p}$ for all $\mathfrak{p}$. In other words $S(J)$ is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^m$ which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{m-1}$. Hence $|J|=2^{m-1}$.

For the next theorem we need,

Remark 2.13. (a) For all nonzero prime ideals $\mathfrak{p}$, the second residue homomorphism $\partial_{\mathfrak{p}}$ maps $I^2F_{\mathfrak{p}}$ onto $I\bar{F}_{\mathfrak{p}}$.

(b) For all dyadic primes $\mathfrak{p}$, $I\bar{F}_{\mathfrak{p}}=(0)$ and hence $\partial_{\mathfrak{p}}$ maps $I^2F_{\mathfrak{p}}$ onto (0).

(c) For all odd primes $\mathfrak{p}$, $I\bar{F}_{\mathfrak{p}} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}$ and the following statement holds: For $\omega \in I^2F_{\mathfrak{p}}$, $S_{\mathfrak{p}}(\omega)=1$ if and only if $\partial_{\mathfrak{p}}(\omega)=0$.

THEOREM 2.14. *Let δ be the number of dyadic primes $\mathfrak{p}_i$ for which -1 is not a square in $F_{\mathfrak{p}_i}$ $(1 \leqslant i \leqslant \delta)$. Then,*

$$|2 \cdot \mathfrak{n}(WF) \cap \mathfrak{n}(WD)| = \begin{cases} 1 & \text{if } \delta = 0, \\ 2^{\delta-1} & \text{if } \delta \geqslant 1. \end{cases}$$

Proof. Let $J=\{\omega \in I^2F \cap \mathfrak{n}(WF) \mid S_{\mathfrak{p}}(\omega)=1 \text{ for all } \mathfrak{p} \neq \mathfrak{p}_i,\ 1 \leqslant i \leqslant \delta\}$. We claim that $J=2 \cdot \mathfrak{n}(WF) \cap \mathfrak{n}(WD)$. We have $2 \cdot \mathfrak{n}(WF) \cap \mathfrak{n}(WD) \subset 2 \cdot \mathfrak{n}(WF) \subset I^2F \cap \mathfrak{n}(WF)$. Also $\omega \in I^2F \cap \mathfrak{n}(WF) = I^2F \cap \ker \sigma \Leftrightarrow \omega \in I^2F$ and $\sigma(\omega)=0$. Therefore $\omega \in 2 \cdot \mathfrak{n}(WF) \Leftrightarrow \omega \in I^2F$, $\sigma(\omega)=0$, and $S_{\mathfrak{p}}(\omega)=1$ for all $\mathfrak{p}$ for which -1 is a square in $F_{\mathfrak{p}}$ (cf. (2.11)). Also $\omega \in I^2F \cap WD \Leftrightarrow \omega \in I^2F$ and $\omega \in \ker \partial_{\mathfrak{p}}$ for all odd $\mathfrak{p}$, (in view of (2.13)(b)) $\Leftrightarrow \omega \in I^2F$ and $S_{\mathfrak{p}}(\omega)=1$ for all odd $\mathfrak{p}$ (cf. (2.13)(c)). Therefore $\omega \in 2 \cdot \mathfrak{n}(WF) \cap \mathfrak{n}(WD) = 2 \cdot \mathfrak{n}(WF) \cap WD \Leftrightarrow \omega \in I^2F$, $\sigma(\omega)=0$, $S_{\mathfrak{p}}(\omega)=1$ for all odd $\mathfrak{p}$ or $\mathfrak{p}$ for which -1 is a square in $F_{\mathfrak{p}} \Leftrightarrow \omega \in I^2F \cap \mathfrak{n}(WF)$, and $S_{\mathfrak{p}}(\omega)=1$ for all $\mathfrak{p} \neq \mathfrak{p}_i$, $1 \leqslant i \leqslant \delta \Leftrightarrow \omega \in J$. This proves our claim, and by (2.12), the theorem follows.

COROLLARY 2.15. *The subgroup $\mathfrak{n}(WD)$ is a direct summand of $\mathfrak{n}(WF)$ if and only if $s+t=\delta-1$ where s, t are as in (2.1) and δ is the number of dyadic primes $\mathfrak{p}$ for which -1 is not square in $F_{\mathfrak{p}}$.*

Proof. Follows from (2.8), (2.10), and (2.14).

In what follows we shall find an upper bound for the order of the group $2 \cdot \mathfrak{n}(WD)$ in terms of the dyadic primes which ramify in $K=F(\sqrt{-1})$.

LEMMA 2.16. *Let L be a local field of characteristic $\neq 2$ and let $M=L(\sqrt{-1})$ be unramified over L. If $N: M^{\cdot} \to L^{\cdot}$ is the norm homomorphism, then $N(U_M)=U_L$.*

Proof. See [2, p. 29].

THEOREM 2.17. *Let F be a number field and let $K=F(\sqrt{-1})$. Let g be*

the number of dyadic primes which are unramified and nonsplit in K (so that $g \leqslant \delta$, δ as in (2.14)). Then,

$$|2 \cdot n(WD)| = 1 \qquad \text{if} \quad g = \delta,$$
$$\leqslant 2^{\delta - g - 1} \qquad \text{if} \quad \delta - g \geqslant 1.$$

Proof. If $\delta = 0$, $2 \cdot n(WD)$ is trivial since $2 \cdot n(WF) \cap WD$ is trivial by (2.14). So let $\delta \geqslant 1$. Consider the image of $2 \cdot n(WD)$ under the homomorphism $S: 2 \cdot n(WF) \cap n(WD) \to (\mathbb{Z}/2\mathbb{Z})^{\delta}$ described in (2.12), (2.14). If $\omega = 2\langle 1, -\lambda \rangle$, with $\langle 1, -\lambda \rangle \in n(WD)$, then $(\lambda) = \mathfrak{a}^2$ for some fractional ideal $\mathfrak{a}$ of F so that $\lambda = u_{\mathfrak{p}} \pi_{\mathfrak{p}}^{2n}$ in $F_{\mathfrak{p}}$ for all nonarchimedean primes $\mathfrak{p}$, where $\pi_{\mathfrak{p}}$ denotes a parameter in $F_{\mathfrak{p}}$. By (2.16), $u_{\mathfrak{p}}$ is a norm from $F_{\mathfrak{p}}(\sqrt{-1})$ for all dyadic primes $\mathfrak{p}$ for which $F_{\mathfrak{p}}(\sqrt{-1})$ is unramified over $F_{\mathfrak{p}}$ and hence $\lambda \in F_{\mathfrak{p}}^{\cdot}$ is a norm from $F_{\mathfrak{p}}(\sqrt{-1})$ for all such $\mathfrak{p}$. This implies $\langle 1, -\lambda, 1, -\lambda \rangle$ is hyperbolic over $F_{\mathfrak{p}}$ for all $\mathfrak{p}$ for which $F_{\mathfrak{p}}(\sqrt{-1})/F_{\mathfrak{p}}$ is unramified. That is, $S_{\mathfrak{p}_i}(\omega) = 1$ for $i = 1, \ldots, g$ (where $F_{\mathfrak{p}_i}(\sqrt{-1})/F_{\mathfrak{p}_i}$ is unramified). Hence $S(2 \cdot n(WD)) \subset (\mathbb{Z}/2\mathbb{Z})^{\delta - g}$. By Hilbert's reciprocity law, $S(2 \cdot n(WD))$ is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^{\delta - g}$, of order $\leqslant \delta - g - 1$; i.e., $|2 \cdot n(WD)| \leqslant 2^{\delta - g - 1}$.

COROLLARY 2.18. (a) *If $\delta = 0$ or 1, $n(WD) \subsetneq n(WF)$ splits.*

(b) *If $\delta \geqslant 2$ and $g \geqslant 1$, $n(WD) \subsetneq n(WF)$ does not split.*

Proof. By (2.10), $n(WD) \subsetneq n(WF)$ splits if and only if $|2 \cdot n(WD)| = |2 \cdot n(WF) \cap n(WD)|$. By (2.14), $|2 \cdot n(WF) \cap n(WD)| = 1$ if $\delta = 0$ and $|2 \cdot n(WF) \cap n(WD)| = 2^{\delta - 1}$ if $\delta \geqslant 1$, which shows that $|2 \cdot n(WD)| = |2 \cdot n(WF) \cap n(WD)|$ if $\delta = 0$ or 1 and that $|2 \cdot n(WD)| < |2 \cdot n(WF) \cap n(WD)|$ if $\delta \geqslant 2$ and $g \geqslant 1$, by (2.17). This proves (a) and (b).

Remark 2.19. In Section 5, we shall consider some examples of cubic fields and compute the integers s and t. However, we note here the following example of a cubic field which illustrates the utility of the above corollary.

EXAMPLE. Let $f(X) = X^3 - 9X^2 - 3X + 3$. This polynomial is irreducible over $\mathbb{Q}$ (Eisenstein!). Let θ be a root of $f(X)$ and let $F = \mathbb{Q}(\theta)$. The polynomial $f(X)$ splits into two irreducible factors over $\mathbb{Q}_2$ (in view of Hensel's lemma; cf. [4, p. 67, 5.23]). Moreover it can be easily seen that $F_1 \simeq \mathbb{Q}_2$ and $F_2 \simeq \mathbb{Q}_2(\sqrt{3})$ where F_i $(i = 1, 2)$ denote the dyadic completions. Both the extensions $F_1(\sqrt{-1})/F$ and $F_2(\sqrt{-1})/F$ are proper and the latter is unramified. Thus we have $\delta = 2$ and $g = 1$. Hence by (2.18), $n(WD) \subsetneq n(WF)$ does not split. In fact in the next section (cf. (3.3)) we shall show that this implies that $WD \subsetneq WF$ does not split.

3. The Structure of the Group $WD \subsetneq WF$

In this section we give the structure of WD as well as some necessary and sufficient conditions for the splitting of $WD \subsetneq WF$.

We first consider the case when F has at least one real completion, i.e., $r \geqslant 1$. In this case the kernel of the signature homomorphism $\sigma: WF \to \coprod_r W\mathbb{R}$ is the nilradical of WF. Hence $\mathfrak{n}(WD) = \mathfrak{n}(WF) \cap WD = W_t F \cap WD$ is the torsion subgroup of WD, which we denote by $W_t D$. Also $\sigma(WD)$ is a free abelian group of rank r (cf. (1.11)). We thus have,

THEOREM 3.1. *If F has at least one real completion, then WD is a direct sum of a free abelian group of rank r and a finite abelian group which is isomorphic to $(\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^u$ with $2s + 2t + u = c + l + d - 1$; c, l, d being as in Section 1 and s, t, and u as in Section 2.*

Proof. By the above discussions it is clear that $WD \backsimeq \sigma(WD) \oplus W_t D \backsimeq \mathbb{Z}^r \oplus W_t D$. By (2.1), $W_t D \backsimeq (\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^u$. Hence $WD \backsimeq \mathbb{Z}^r \oplus (\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^u$.

We continue to assume $r \geqslant 1$ and go on to the question of the splitting of $WD \subsetneq WF$. We begin with the following lemma.

LEMMA 3.2. *Let G' be an abelian group of rank n and let G be a finitely generated subgroup of G', having the same rank. Let G'_t, G_t denote their respective torsion subgroups. Then G is a direct summand of G' if and only if the following two conditions are satisfied*: (i) *G_t is a direct summand of G'_t*, (ii) *the induced map $G/G_t \to G'/G'_t$ is surjective.*

Proof. Let (i) and (ii) hold. Since $G_t = G \cap G'_t$, the natural map $G/G_t \to G'/G'_t$ is injective. Thus (ii) implies that this is in fact an isomorphism. Let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis of $G/G_t \backsimeq G'/G'_t$ with $e_1, \ldots, e_n$ in G. Then, $G = G_t \oplus \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ and $G' = G'_t \oplus \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$. Let $\varepsilon: G'_t \to G_t$ be a section to $G_t \subsetneq G'_t$. Then the map $\eta: G' \to G$ given by $\eta(x, \alpha_1 e_1, \ldots, \alpha_n e_n) = (\varepsilon(x), \alpha_1 e_1, \ldots, \alpha_n e_n)$ gives a section to $G \subsetneq G'$. Hence G is a direct summand of G'.

Conversely suppose G is a direct summand of G'. Let $\eta: G' \to G$ be a section to $G \subsetneq G'$. Restricting η to G'_t we get a section $\eta/G'_t: G'_t \to G_t$, to $G_t \subsetneq G'_t$; i.e., G_t is a direct summand of G'_t. This implies (i). Also, η induces a homomorphism $\tilde{\eta}: G'/G'_t \to G/G_t$. Clearly the composition $G/G_t \to G'/G'_t \to^{\tilde{\eta}} G/G_t$ is identity on G/G_t. Since both G/G_t and G'/G'_t are free of the same rank, it follows that $G/G_t \to G'/G'_t$ is an isomorphism. This implies (ii), and proves the converse.

COROLLARY 3.3. *If F is a number field with at least one real completion, then $WD \subsetneq WF$ splits if and only if the following two conditions are satisfied:*

(i) *$W_tD \subsetneq W_tF$ splits,*

(ii) *$\sigma(WD) = \sigma(WF)$, where $\sigma: WF \to \bigsqcup_r W\mathbb{R}$ is the total signature homomorphism.*

Proof. We recall that $W_tF = \ker \sigma$, $W_tD = \ker \sigma \cap WD$, and that WD is a finitely generated subgroup of WF having the same rank as WF (cf. (3.1)). Hence we have a commutative diagram,

$$\begin{array}{ccc} WD/W_tD & \longrightarrow & WF/W_tF \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ \sigma(WD) & \longrightarrow & \sigma(WF) \end{array}$$

Thus condition (ii) of (3.2) is equivalent to the condition $\sigma(WD) = \sigma(WF)$. Hence the corollary follows.

For later use we discuss here a necessary and sufficient condition for the equality $\sigma(WD) = \sigma(WF)$.

PROPOSITION 3.4. *Let $r \geqslant 1$ and let $F_1, \ldots, F_r$ denote the real completions of F. Then $\sigma(WD) = \sigma(WF)$ if and only if there exist $\lambda_2, \ldots, \lambda_r$ in F such that for all i, λ_i is negative in F_i and positive in F_j for all $j \neq i$, and such that $(\lambda_i) = \mathfrak{a}_i^2$ for some fractional ideal $\mathfrak{a}_i$ of F $(2 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant r)$.*

Proof. By the approximation theorem on absolute values, there exist $\lambda_2, \ldots, \lambda_r$ in F such that $2 \leqslant i \leqslant r$, λ_i is negative in F_i and positive in F_j for all $j \neq i$, $1 \leqslant j \leqslant r$. From this it follows (cf. [7, p. 172, 3.9]) that $\sigma(WF)$ is generated freely by $\{\langle\sigma(1)\rangle, \langle\sigma(\lambda_2)\rangle, \ldots, \langle\sigma(\lambda_r)\rangle\}$. If λ_i can further be chosen so that $(\lambda_i) = \mathfrak{a}_i^2$ for some ideal $\mathfrak{a}_i$ of F $(2 \leqslant i \leqslant r)$, clearly $\sigma(WD) = \sigma(WF)$. Conversely suppose $\sigma(WD) = \sigma(WF)$. Then there exists $q_i \in WD$ such that $\sigma(q_i) = \sigma(\langle\lambda_i\rangle)$, $2 \leqslant i \leqslant r$. The claim that λ_i can further be chosen so that $(\lambda_i) = \mathfrak{a}_i^2$ $(2 \leqslant i \leqslant r)$ follows from the following fact: If $\tau: F \to \mathbb{R}$ is any real imbedding and for $q \in WF$, $\tau(q) = \langle \pm 1 \rangle$ then $\tau(\langle \mathfrak{d}(q) \rangle) = \tau(q)$, where $\mathfrak{d}$ denotes the (signed) discriminant of q.

We now consider the case when F is totally imaginary, i.e., $r = 0$. In this case $\eta(WD) = IF \cap WD$ and we denote it by ID. We have an exact sequence

$$0 \longrightarrow IF \longrightarrow WF \xrightarrow{e} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

where e is the dimension index function (cf. [8, p. 66, 3.3]). By restricting e to WD, we get an exact sequence

$$0 \longrightarrow ID \longrightarrow WD \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \qquad (**)$$

We note that in this case $W_t F = WF$, since F has no real completions and in contrast to the earlier case, WF may have elements of order 8. (However, $8 \cdot WF \subset I^3 F = (0)$). The sequence $(**)$ describes WD as an extension of $\mathbb{Z}/2\mathbb{Z}$ by ID, whose structure is already determined in (2.1). The following theorem gives a more precise description of WD.

The next results need the notion of level of fields. For the definition cf. [11, p. 71, 10.6]. We remark that the level $\tilde{s}(F)$ of a totally imaginary number field F is 2^n, with $n \leqslant 2$.

THEOREM 3.5. *Let F be a totally imaginary number field. Let $\tilde{s}(F)$ denote the level of F. Then we have,*

(i) $WD \simeq \mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})^{s+t-1} \oplus (\mathbb{Z}/2\mathbb{Z})^u$, *if* $\tilde{s}(F) = 4$.

(ii) $WD \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t+1} \oplus (\mathbb{Z}/2\mathbb{Z})^{u-1}$, *if* $\tilde{s}(F) = 2$.

(iii) $WD \simeq (\mathbb{Z}/2\mathbb{Z})^{c+l+d}$ *if* $\tilde{s}(F) = 1$ *where s, t, u, c, l, and d are as in* (2.1).

Proof. (i) Let $\tilde{s}(F) = 4$. Then -1 is not a sum of two squares in F, and hence $\langle 1, 1, 1, 1 \rangle$ is anisotropic over F. Therefore $\langle 1 \rangle$ is an element of order 8 in WD (since $8 \cdot WD \subset 8 \cdot WF = (0)$). Hence $WD \simeq (\langle 1 \rangle) \oplus WD/(\langle 1 \rangle)$ where $(\langle 1 \rangle)$ denotes the cyclic subgroup of WD generated by $\langle 1 \rangle$, which is of order 8. Now, the natural map $ID \to WD/(\langle 1 \rangle)$ has kernel $ID \cap (\langle 1 \rangle) = (\langle 1, 1 \rangle)$ so that $ID/(\langle 1, 1 \rangle) \subseteq WD/(\langle 1 \rangle)$. A comparison of the orders of these groups shows that this is in fact an isomorphism. Thus $WD/(\langle 1 \rangle) \simeq ID/(\langle 1, 1 \rangle)$. Since $4 \cdot ID \subset (4 \cdot IF \subset I^3 F) = (0)$, and $\langle 1, 1 \rangle$ is an element of order 4 in ID, we have $ID \simeq (\langle 1, 1 \rangle) \oplus ID/(\langle 1, 1 \rangle)$. Also $ID \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^u$ by (2.1). This shows that $ID/(\langle 1, 1 \rangle) \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t-1} \oplus (\mathbb{Z}/2\mathbb{Z})^u$. Hence $WD \simeq \mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/4\mathbb{Z})^{s+t-1} \oplus (\mathbb{Z}/2\mathbb{Z})^u$.

(ii) Let $\tilde{s}(F) = 2$. In this case $4 \cdot WD = (0)$ and $\langle 1 \rangle$ is an element of order 4 in WD. Hence $WD \simeq (\langle 1 \rangle) \oplus WD/(\langle 1 \rangle)$ (where $(\langle 1 \rangle)$ is the cyclic subgroup of WD generated by $\langle 1 \rangle$). As in case (i), we have $ID/(\langle 1, 1 \rangle) \simeq WD/(\langle 1 \rangle)$. However, in this case we claim that $ID/(\langle 1, 1 \rangle) \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^{u-1}$. For, to find the number of $\mathbb{Z}/4\mathbb{Z}$ components of $ID/(\langle 1, 1 \rangle)$, it is enough to find the order of $2 \cdot (ID/(\langle 1, 1 \rangle))$, by (2.2). Consider the natural map $2 \cdot ID \to 2 \cdot (ID/(\langle 1, 1 \rangle))$ which is defined by $\langle 1, \lambda, 1, \lambda \rangle \to \langle \overline{1, \lambda, 1, \lambda} \rangle$ (cf. (1.10)). This is clearly a surjective homomorphism. We claim that it is injective. For $\langle \overline{1, \lambda, 1, \lambda} \rangle = 0$ implies

that $\langle 1, \lambda, 1, \lambda \rangle \in (\langle 1, 1 \rangle)$ (which is a group of order 2). Since -1 is not a square in F, $\langle 1, \lambda, 1, \lambda \rangle \neq \langle 1, 1 \rangle$ so that $\langle 1, \lambda, 1, \lambda \rangle = 0$. Thus we have $|2 \cdot (ID/(\langle 1, 1 \rangle))| = |2 \cdot ID| = 2^{s+t}$, so that $ID/(\langle 1, 1 \rangle) \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t} \oplus (\mathbb{Z}/2\mathbb{Z})^{u-1}$ and $WD \simeq (\mathbb{Z}/4\mathbb{Z})^{s+t+1} \oplus (\mathbb{Z}/2\mathbb{Z})^{u-1}$.

(iii) Since $\tilde{s}(F) = 1$, -1 is a square in F and hence WD is 2-torsion and $WD \simeq (\mathbb{Z}/2\mathbb{Z})^{c+l+d}$, in view of (1.11).

We finally take up the question of the splitting of $WD \subsetneq WF$, in the case $r = 0$. We have,

THEOREM 3.6. *Let F be a totally imaginary number field. Then the following statements are equivalent*:

(i) *$WD \subsetneq WF$ splits.*

(ii) *$ID \subsetneq IF$ splits.*

(iii) *Every element of WD which is 2-divisible in WF, is 2-divisible in WD.*

Proof. (Recall: (i) is equivalent to WD being a pure subgroup of WF (cf. (2.9))). We prove (i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (ii). (iii) $\Rightarrow$ (i). We have three cases to consider: (a) $\tilde{s}(F) = 1$. In this case $2 \cdot WF = 0$ and the claim is obvious. (b) $\tilde{s}(F) = 2$. In this case $4 \cdot WF = (0)$ and (iii) implies that WD is a pure subgroup of WF, so that (i) follows from (2.9). (c) $\tilde{s}(F) = 4$. In this case $8 \cdot WF = (0)$. Hence to prove purity of WD in WF it is enough to prove that every element of WD which is 4-divisible in WF is 4-divisible in WD. So, let $\omega = 4\langle a_1, \ldots, a_n \rangle$, $a_i \in F^*$. Since $4\langle a_i \rangle \simeq 4\langle 1 \rangle$ (cf. (1.8), (1.9)), $\omega = 4\langle 1, \ldots, 1 \rangle$ which shows that ω is 4-divisible in WD. Thus (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (iii) is trivial.

(ii) $\Rightarrow$ (iii). Let $\omega \in WD$ and let $\omega = 2 \cdot q$, $q \in WF$. If $\dim q$ is even,

(ii) implies that $\omega = 2 \cdot q'$, $q' \in ID \subset WD$. Suppose $\dim q$ is odd. Then $\omega \perp \langle 1, 1 \rangle = 2(q \perp \langle 1 \rangle)$, where $q \perp \langle 1 \rangle \in IF$ and by (ii) $\omega \perp \langle 1, 1 \rangle = 2 \cdot q'$, $q' \in ID$. Hence $\omega = \omega \perp 2\langle 1, -1 \rangle = 2(q' \perp \langle -1 \rangle)$ where $q' \perp \langle -1 \rangle \in WD$. This implies (iii).

(iii) $\Rightarrow$ (ii). Let $\omega \in ID$ and let $\omega = 2 \cdot q$, $q \in IF$. Then (iii) implies that $\omega = 2 \cdot q'$, $q' \in WD$. Hence $\mathfrak{d}(\omega) = (-1)^{\dim q'}$. Also $\omega \in 2 \cdot IF \subset I^2F$ implies that $\mathfrak{d}(\omega) = 1$. Hence if $\tilde{s}(F) \neq 1$, $\dim q'$ is even, so that $\omega \in 2 \cdot ID$, and (ii) follows. (Note that $4 \cdot IF = (0)$.) If $\tilde{s}(F) = 1$, the assertion is obvious.

COROLLARY 3.7. *Let F be totally imaginary. Then $WD \subsetneq WF$ splits if and only if $s + t = \delta - 1$, where s, t, and δ are as in Section 2.*

Proof. Follows from (2.15) and (3.6).

4. Quadratic Fields

Let $F=\mathbb{Q}(\sqrt{m})$ and let Δ be the discriminant of F. In this section we determine the structure of WD and give a necessary and sufficient condition for the splitting of $WD \subsetneq WF$ in terms of the prime divisors of the discriminant, in the case when F is real. When F is imaginary, we show that $WD \subsetneq WF$ always splits.

We note that $\Delta = m$ or $4m$ according to whether m is congruent to 1 mod 4 or m is congruent to 2 or 3 mod 4. We also recall the following elementary results from algebraic number theory. The proofs of these results can be found in [9] or [5].

Lemma 4.1. *The prime ideal* (2) *splits in* F *if and only if* Δ *is congruent to* 1 mod 8.

Proof. See [9, p. 166, 4.13].

Lemma 4.2. *Let* $\mathbf{v}$ *be the number of distinct prime divisors of* Δ. *Then* $|{}_2H^*(F)| = 2^{\mathbf{v}-1}$, *where* $H^*(F)$ *is the ideal class group in the narrow sense.*

Proof. See [5, pp. 516, 582].

We first consider the case of a real quadratic field; i.e., $F=\mathbb{Q}(\sqrt{m})$, $m>0$. Let $K=F(\sqrt{-1})$.

Proposition 4.3. *Let* $F=\mathbb{Q}(\sqrt{m})$, $m>0$, *and let* Δ *be congruent to* 1 mod 8. *If* Δ *has no prime divisor congruent to* 3 mod 4, *then we have* (a) $U_F^+ \subset N(K)$ *and* (b) $\mathscr{H} = {}_2H^*(F)$ ($\mathscr{H}$ *as defined in* (2.1)).

Proof. (a) By Dirichlet's theorem on units, U_F is the direct product of a free abelian group of rank 1 and the group $\{1, -1\}$, since F is real quadratic. Let u be a free generator of U_F. If $N_{F/Q}(u) = -1$, then every element of U_F^+ is a square and hence belongs to $N(K)$. Suppose $N_{F/Q}(u) = 1$. By replacing u by $-u$ if necessary we may assume that $u \in U_F^+$. By Hilbert's theorem 90, there exists η in F such that $u = \eta(\sigma(\eta))^{-1}$ where σ is the nontrivial automorphism of $F/\mathbb{Q}$. In fact we choose $\eta = \sqrt{\Delta}(1-u)$. Then u and $N_{F/\mathbb{Q}}(\eta)$ are in the same class in F^*/F^{*2}. We have $N(\eta) = \Delta(1-u)^2/u > 0$ and the ideal (η) is invariant under σ. Thus $(\eta) = (n)\,\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_{\mathbf{v}}^{a_{\mathbf{v}}}$ where the $\mathfrak{p}_i$ are ramified prime ideals of $F/\mathbb{Q}$, $a_i = 0$ or 1, and $n \in \mathbb{Q}$. Hence $N(\eta) = n^2 \cdot p_1^{a_1} \cdots p_{\mathbf{v}}^{a_{\mathbf{v}}}$ (since $N(\eta) > 0$) where $a_i = 0$ or 1 and $p_1, \ldots, p_{\mathbf{v}}$ are prime divisors of Δ. Since Δ has no prime divisor congruent to 3 mod 4, this shows that $N_{F/\mathbb{Q}}(\eta)$ is up to squares a product of primes of $\mathbb{Q}$ which are congruent to 1 mod 4 and hence a sum of two squares in $\mathbb{Q}$. This implies that u is a norm from $K = F(\sqrt{-1})/F$. Hence $U_F^+ \subset N(K)$. (b) The group

${}_2H^*(F)$ is generated by the class of $\mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_{\mathfrak{v}}^{a_{\mathfrak{v}}}$, where $\Delta = p_1\cdots p_{\mathfrak{v}}$, $\mathfrak{p}_i/p_i$, and $a_i = 0$ or 1 $(1 \leqslant i \leqslant \mathfrak{v})$ (cf. [9, p. 392]). Thus $\tilde{\mathfrak{a}} \in {}_2H^*(F)$ implies that $\mathfrak{a}^2 = (\lambda^2 p_{i_1}\cdots p_{i_n})$, $n \leqslant \mathfrak{v}$. Since any such element is up to squares an integer congruent to 1 mod 4, we have $\mathfrak{a}^2 = (N(\mu))$ for some $\mu \in K^*$. Hence $\tilde{\mathfrak{a}} \in \mathscr{H}$, which implies that ${}_2H^*(F) = \mathscr{H}$. This proves (b).

PROPOSITION 4.4. *Let $F = \mathbb{Q}(\sqrt{m})$, $m > 0$. Then $|2 \cdot W_t D| = 2$ if and only if the following two conditions are satisfied:*

(i) *Δ is congruent to* 1 mod 8.

(ii) *Δ has a prime divisor p, which is congruent to* 3 mod 4.

Proof. Suppose (i) and (ii) hold. By (4.1), F has two dyadic primes. Since $[F: \mathbb{Q}] = 2$, both the dyadic completions are isomorphic to $\mathbb{Q}_2$. Let p divide Δ and let p be congruent to 3 mod 4. Then $(p) = \mathfrak{p}^2$ in F and hence $\langle 1, -p\rangle$ is in $W_t D$ by (2.4). Since p is congruent to 3 mod 4, p is not a sum of two squares in $\mathbb{Q}_2$. Hence $\langle 1, -p, 1, -p\rangle$ is anisotropic over $\mathbb{Q}_2$, so that it is anisotropic over F. Thus $|2 \cdot W_t D| \geqslant 2$. By (2.18), $|2 \cdot W_t D| \leqslant 2$ and hence $|2 \cdot W_t D| = 2$.

Conversely, if Δ is not congruent to 1 mod 8, then there exists only one dyadic prime and hence $\delta = 0$ or 1. By (2.18), $|2 \cdot W_t D| = 1$. If Δ is congruent to 1 mod 8 and Δ has no prime divisor which is congruent to 3 mod 4, then $U_F^+ \subset N(K)$ and $\mathscr{H} = {}_2H^*(F)$ (cf. (4.3)); i.e., $s = 0$ and $t = 0$ in the notation of Section 2. Thus $|2 \cdot W_t D| = 1$ and the converse follows.

THEOREM 4.5. *Let $F = \mathbb{Q}(\sqrt{m})$, $m > 0$, and let Δ be its discriminant. Let $\mathfrak{v}$ be the number of distinct prime divisors of Δ. Then we have,*

(i) $WD \simeq \mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-1}$, *if Δ is not congruent to* 1 mod 8.

(ii) $WD \simeq \mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}}$, *if Δ is congruent to* 1 mod 8 *and Δ has no prime divisor congruent to* 3 mod 4.

(iii) $WD \simeq \mathbb{Z}^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-2}$, *if Δ is congruent to* 1 mod 8 *and Δ has a prime divisor congruent to* 3 mod 4.

Proof. In view of (3.1), it is enough to compute $W_t D$. We have $c = 0$ and $l = \mathfrak{v} - 1$ by (4.2). If Δ is not congruent to 1 mod 8 then $d = 1$ by (4.1). Thus $|W_t D| = 2^{\mathfrak{v}-1}$ and $|2 \cdot W_t D| = 1$ by (2.17), so that $W_t D \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-1}$, in view of (2.2). This proves (i). Next let Δ be congruent to 1 mod 8. Then we have $d = 2$ so that $|W_t D| = 2^{l+1} = 2^{\mathfrak{v}}$. By (2.2) and (4.4), it follows that $W_t D \simeq (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}}$, if Δ has no prime divisor congruent to 3 mod 4, and $W_t D \simeq \mathbb{Z}(4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-2}$, if Δ has a prime divisor congruent to 3 mod 4. This proves (ii) and (iii).

PROPOSITION 4.6. *Let* $F=\mathbb{Q}(\sqrt{m})$, $m>0$. *Then* $W_tD \subsetneq W_tF$ *splits if only if one of the following two conditions holds*:

(i) Δ *is not congruent to* 1 mod 8.

(ii) Δ *is congruent to* 1 mod 8 *and* Δ *has a prime divisor* p, *which is congruent to* 3 mod 4.

Proof. Suppose (i) holds. Then $d=1$, so that $\delta=0$ or 1. Hence $|2\cdot W_tF\cap W_tD|=1=|2\cdot W_tD|$. If (ii) holds, then $|2W_tF\cap W_tD|=2$ and $|2\cdot W_tD|=2$ by (4.4), so that $|2\cdot W_tF\cap W_tD|=|2\cdot W_tD|$. Hence in either case, $W_tD\subsetneq W_tF$ splits.

Conversely, let $W_tD\subsetneq W_tF$ split. If Δ is congruent to 1 mod 8, $|2\cdot W_tF\cap W_tD|=2$ and hence by (2.10), $|2\cdot W_tD|=2$. This implies, in view of (4.4), that Δ has a prime divisor $p\equiv 3$ mod 4, i.e., (ii) holds.

PROPOSITION 4.7. *Let* $F=\mathbb{Q}(\sqrt{m})$, $m>0$, *and* let $\sigma: WF\to \coprod_{r=2} W\mathbb{R}$ *be the total signature homomorphism. Then the following four conditions are equivalent*:

(1) $\sigma(WD)=\sigma(WF)$.

(2) *There exists* λ *in* $F^{\cdot}$ *such that* $N_{F/\mathbb{Q}}(\lambda)$ *is negative and* $(\lambda)=\mathfrak{a}^2$ *for some fractional ideal* $\mathfrak{a}$ *of* F.

(3) *The form* $\langle 1, 1, -m\rangle$ *is isotropic over* $\mathbb{Q}$.

(4) *The discriminant* Δ *of* F *has no prime divisor* p, *which is congruent to* 3 mod 4.

Proof. The equivalence of (1) and (2) is established in (3.4).

(2) $\Rightarrow$ (3). Let $\lambda\in F^{\cdot}$, $(\lambda)=\mathfrak{a}^2$, for a fractional ideal $\mathfrak{a}$ of F, and let $N_{F/\mathbb{Q}}(\lambda)$ be negative. Then $(N_{F/\mathbb{Q}}(\lambda))=(a^2)$ for some a in $\mathbb{Q}$, so that $N_{F/\mathbb{Q}}(\lambda)=-a^2$. This implies that the equation $X^2-mY^2=-1$ has a rational solution; i.e., $\langle 1, 1, -m\rangle$ is isotropic over $\mathbb{Q}$.

(3) $\Rightarrow$ (2). $\langle 1, 1, -m\rangle$ is isotropic over $\mathbb{Q}$ implies that $X^2-mY^2=-1$ has a rational solution, so that there exists λ in F with $N_{F/\mathbb{Q}}(\lambda)=-1$. Let $(\lambda)=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_k^{e_k}$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are distinct prime ideals of F and $e_i\neq 0$ for any $i=1, \ldots, k$. Since, $\lambda\sigma(\lambda)=-1$, we have $\mathfrak{p}_1^{-e_1}\cdots\mathfrak{p}_k^{-e_k}=\sigma(\mathfrak{p}_1)^{e_1}\cdots\sigma(\mathfrak{p}_k)^{e_k}$. Thus for every i, $\mathfrak{p}^{-e_i}=\sigma(\mathfrak{p}_j)^{e_j}$ for some j. Since $e_i\neq 0$, we have $j\neq i$ for any such pair (i, j). Hence k is even and we have

$$\begin{aligned}(\lambda) &= \mathfrak{p}_1^{e_1}\sigma(\mathfrak{p}_1)^{e_1}\cdots\mathfrak{p}_n^{e_n}\sigma(\mathfrak{p}_n)^{-e_n}\\ &= (\mathfrak{p}_1^{e_1}\sigma(\mathfrak{p}_1)^{e_1})\cdots(\mathfrak{p}_n^{e_n}\sigma(\mathfrak{p}_n)^{e_n})(\sigma(\mathfrak{p}_1)^{-2e_1}\cdots\sigma(\mathfrak{p}_n)^{-2e_n})\\ &= (\alpha)\,\mathfrak{a}^2,\end{aligned}$$

where $\alpha \in \mathbb{Q}^*$ and $\mathfrak{a}$ is a fractional ideal of F. Thus we have, if $\mu = \alpha\lambda$, that $N_{F/\mathbb{Q}}(\mu)$ is negative and $(\mu) = \mathfrak{a}^2$ for some fractional ideal $\mathfrak{a}$ of F, which implies (2).

(3) $\Leftrightarrow$ (4). Since Δ and m are in the same class in F^*/F^{*2}, $\langle 1, 1, -m \rangle$ is isotropic over $\mathbb{Q}$ if and only if $\langle 1, 1, -\Delta \rangle$ is isotropic. However a square-free positive integer a is a sum of two squares in $\mathbb{Q}$ if and only if no prime p which is congruent to 3 mod 4, divides a. This proves our assertion.

THEOREM 4.8. *Let* $F = \mathbb{Q}(\sqrt{m})$, $m > 0$. *Then the exact sequence* $0 \to WD \to WF$ *splits if and only if the following two conditions hold:*

(1) Δ *is not congruent to* 1 mod 8.

(2) Δ *has no prime divisor* p, *which is congruent to* 3 mod 4.

Proof. Follows from (3.3), (4.6), and (4.7).

We now give some simple consequences of our results in the real quadratic case.

LEMMA 4.9. *Let* $F = \mathbb{Q}(\sqrt{p})$ *where* p *is a prime. Then* $|H(F)|$ *is odd, where* $H(F)$ *is the ideal class group of* F.

Proof. We recall that $H^*(F)$ is the ideal class group of F in the narrow sense and that $H(F)$ is the ideal class group in the usual sense. Thus we have a natural homomorphism f: $H^*(F) \to H(F)$ which is surjective, so that $H^*(F)/\ker f \cong H(F)$. Clearly, $\ker f \subset {}_2H^*(F)$. If $p = 2$ or p is congruent to 1 mod 4, then $\Delta = p^a$ ($a = 3$ or 1), and by (4.2) ${}_2H^*(F)$ is trivial, which shows that $|H^*(F)| = |H(F)|$ is odd. If p is congruent to 3 mod 4, the proof of (4.7) above shows that the norm of any unit is positive. We claim that in this case $\ker f$ is nontrivial. By the approximation theorem on absolute values there exists $\lambda \in F^*$, such that $\lambda \cdot \sigma(\lambda)$ is negative. If $\ker f = (0)$, then $(\lambda) = (\mu)$ for some $\mu \in F^+$, so that $\lambda = u \cdot \mu$ for some $u \in U_F$. This implies that $N(u)$ is negative, which is not possible. Hence $\ker f$ is nontrivial. By (4.2), $|{}_2H^*(F)| = 2$ and hence $\ker f = {}_2H^*(F)$. Suppose $x \in H(F)$ is of order 2. Then $x = f(\bar{\mathfrak{a}})$, with $\bar{\mathfrak{a}} \in H^*(F)$, $\bar{\mathfrak{a}}^2 \in \ker f$, $\bar{\mathfrak{a}}^2 \neq 1$ (since otherwise $\bar{\mathfrak{a}} \in {}_2H^*(F) = \ker f$, which would imply that $f(\bar{\mathfrak{a}}) = x = 1$). This implies that $\mathfrak{a}^2 = (\lambda)$, with $N(\lambda) < 0$, contradicting (4.7). Hence $|H(F)|$ is odd.

PROPOSITION 4.10. *Let* $F = \mathbb{Q}(\sqrt{p})$, *where* $p > 0$ *is a prime. Then the sequence*

$$0 \to WD \to WF \to \bigsqcup_{0 \neq \mathfrak{p}} W\bar{F}_{\mathfrak{p}} \to 0 \qquad (***)$$

is exact. It is split exact if and only if $p = 2$ *or* p *is congruent to* 5 mod 8.

Proof. For any number field F, we have an exact sequence

$$0 \to WD \to WF \to \bigsqcup_{0 \neq \mathfrak{p}} W\bar{F}_{\mathfrak{p}} \to H(F)/H(F)^2 \to 0.$$

By (4.9) $H(F)/H(F)^2$ *is trivial for* $F = \mathbb{Q}(\sqrt{p})$. *Hence* (***) *is exact. The splitting condition follows from* (4.8).

Remark 4.11. As a consequence of (4.8) we have infinitely many real quadratic fields F for which $0 \to WD \to WF$ splits and infinitely many quadratic fields for which the sequence does not split. If p is a prime congruent to 1 mod 8 and $F = \mathbb{Q}(\sqrt{p})$, the sequence (***) is exact but not split exact. In particular for $F = \mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\sqrt{41})$, and $\mathbb{Q}(\sqrt{73})$, (***) is exact but not split exact. It is interesting to note that these fields are known to be Euclidean (cf. [9, p. 115, 3.11, p. 132]).

We shall now proceed to consider the imaginary quadratic fields.

THEOREM 4.12. *Let* $F = \mathbb{Q}(\sqrt{m})$, $m < 0$, *and let* Δ *be its discriminant. Let* $\mathfrak{v}$ *be the number of distinct prime divisors of* Δ. *Then we have,*

(1) $WD \simeq (\mathbb{Z}/2\mathbb{Z})^2$ *if* $\Delta = -4$.

(2) $WD \simeq (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-1}$ *if* $\Delta \neq -4$ *and* Δ *is not congruent to* 1 mod 8.

(3) $WD \simeq (\mathbb{Z}/8\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-1}$, *if* Δ *is congruent to* 1 mod 8.

Proof. (1) If $\Delta = -4$, then $F = \mathbb{Q}(\sqrt{-1})$ and we have $c = 1$, $l = \mathfrak{v} - 1 = 0$, $d = 1$. Hence by (3.5) we have $WD \simeq (\mathbb{Z}/2\mathbb{Z})^2$. (2) Let $\Delta \neq -4$ and let Δ be not congruent to 1 mod 8. Then -1 is not a square in F and there is only one dyadic prime of F. Hence $\langle 1, 1, 1, 1 \rangle$ is hyperbolic over F so that $\tilde{s}(F) = 2$. Thus in this case we have, $s + t = 0$, $c = 1$, $d = 1$, and $l = \mathfrak{v} - 1$. By (3.5)(ii), we have $WD \simeq \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-1}$ which proves (2).

(3) Let Δ be congruent to 1 mod 8. Then $d = 2$, and $\langle 1, 1, 1, 1 \rangle$ is anisotropic over both the dyadic completions (both are isomorphic to $\mathbb{Q}_2$), so that $\tilde{s}(F) = 4$. Hence (3.5)(iii) yields $WD \simeq \mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{v}-1}$ (since $c = 1$, $l = \mathfrak{v} - 1$, $d = 2$ in this case).

Finally we prove,

THEOREM 4.13. *Let* $F = \mathbb{Q}(\sqrt{m})$, $m < 0$. *Then,* $0 \to WD \to WF$ *always splits.*

Proof. In view of (3.6), it is enough to prove that every element of ID, which is 2-divisible in IF, is 2-divisible in ID. We have two cases to consider.

TABLE 4.14

Real Quadratic Fields

Nature of Δ	Structure of WD	Splitting of $WD \subsetneq WF$?
$\Delta \not\equiv 1 \bmod 8$ and Δ has no prime divisor $\equiv 3 \bmod 4$	$\mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^{\nu-1}$	Yes
$\Delta \not\equiv 1 \bmod 8$ and Δ has a prime divisor $\equiv 3 \bmod 4$	$\mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^{\nu-1}$	No
$\Delta \equiv 1 \bmod 8$ and Δ has no prime divisor $\equiv 3 \bmod 4$	$\mathbb{Z}^2 \oplus (\mathbb{Z}/2\mathbb{Z})^{\nu}$	No
$\Delta \equiv 1 \bmod 8$ and Δ has a prime divisor $\equiv 3 \bmod 4$	$\mathbb{Z}^2 \oplus \mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\nu-2}$	No

Note. $F = \mathbb{Q}(\sqrt{m})$, $m > 0$, Δ = discriminant of F, ν = number of distinct prime divisors of Δ, D = ring of integers of F, WD = Witt group of D, and WF = Witt group of F.

Case (i): *Δ is not congruent to* 1 mod 8. In this case $d = 1$ and $2 \cdot IF \cap WD$ is trivial. Hence the 2-divisibility condition is trivially satisfied for $ID \subsetneq IF$, and the assertion follows.

Case (ii): *Δ is congruent to* 1 mod 8. In this case $d = 2$ and $2 \cdot IF \cap WD$ is of order 2. Since $\langle 1, 1, 1, 1 \rangle$ is anisotropic, and belongs to $2 \cdot ID$, we have $|2 \cdot ID| = 2$, which proves that $ID \subsetneq IF$ splits. Hence $0 \to WD \to WF$ splits.

We summarise the main results of this section in Table 4.14 and 4.15.

5. Cubic Fields

Let $F = \mathbb{Q}(\sqrt[3]{m})$, where m is a cube-free integer. In this section we calculate the index of $N(K) \cap U_F^+$ in U_F^+ (cf. Sections 1, 2 for notation) for

TABLE 4.15

Imaginary Quadratic Fields

Nature of Δ	Structure of WD	Splitting of $WD \subsetneq WF$?
$\Delta = -4$	$(\mathbb{Z}/2\mathbb{Z})^2$	Yes
$\Delta \neq -4$, $\Delta \not\equiv 1 \bmod 8$	$\mathbb{Z}/4\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\nu-1}$	
$\Delta \equiv 1 \bmod 8$	$\mathbb{Z}/8\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^{\nu-1}$	

Note. $F = \mathbb{Q}(\sqrt{m})$, $m < 0$, Δ = discriminant of F, ν = number of distinct prime divisors of Δ, WF = Witt group of F, WD = Witt group of D, where D = ring of integers of F.

some cubic fields $\mathbb{Q}(\sqrt[3]{m})$ and compute the Witt group of D. We also discuss the question of the splitting of $WD \subsetneq WF$ for these fields.

Remark 5.1. Any cubic field $F = \mathbb{Q}(\sqrt[3]{m})$ has one real completion and one pair of complex completions, i.e., $r = 1$ and $c = 1$. The signature homomorphism $\sigma: WD \to W\mathbb{R}$ is surjective in this case and hence $\sigma(WD) = \sigma(WF)$. Thus $WD \subsetneq WF$ splits if and only if $W_t D \subsetneq W_t F$ splits (cf. (3.3)).

LEMMA 5.2. *Let $F = \mathbb{Q}(\sqrt[3]{m})$ and let d be the number of dyadic primes of F. Then $d = 1$ if m is even and $d = 2$ if m is odd.*

Proof. Consider the cubic polynomial $X^3 - m$ over $\mathbb{Q}_2$. Let $m = 2n$. We claim that $X^3 - 2n$ is irreducible over $\mathbb{Q}_2$. For, suppose theere exists $a \in \mathbb{Q}_2$ such that $a^3 - 2n = 0$. Then 2 divides a^3 in $\mathbb{Z}_2$ so that 2^3 divides a^3 in $\mathbb{Z}_2$; i.e., 2^3 divides m which is a contradiction due to the fact that m is cube free. Hence $X^3 - m$ is irreducible over $\mathbb{Q}_2$ if m is even, so that $d = 1$. On the other hand if m is odd, $X^3 - m = (X - 1)(X^2 + X + 1)$ over the residue class field $\mathbb{Z}/2\mathbb{Z}$. By Hensel's lemma $X^3 - m$ factors over $\mathbb{Q}_2$. Further, $X^2 + X + 1$ being irreducible over $\mathbb{Z}/2\mathbb{Z}$, $X^3 - m$ splits into two irreducible factors over $\mathbb{Q}_2$, i.e., $d = 2$, if m is odd. This proves the lemma.

COROLLARY 5.3. *If δ denotes the number of dyadic primes $\mathfrak{p}$ for which -1 is not a square in $F_{\mathfrak{p}}$, then we have* (i) *$\delta = 2$ if m is odd, and* (ii) *$\delta = 1$ if m is even.*

Proof. If m is odd, $d = 2$ by (5.2) above. Let F_1, F_2 be the dyadic completions of F. Then the proof of the above lemma shows that $F_1 \not\simeq \mathbb{Q}_2$ and F_2 is a quadratic extension of $\mathbb{Q}_2$, with residue class degree 2. Thus 2 is a parameter in both the fields F_1 and F_2. Thus $\delta = 2$, if m is odd. If m is even, $d = 1$ and F_1 is a cubic extension of $\mathbb{Q}_2$ and hence -1 is not a square in F_1, i.e., $\delta = 1$. This proves the corollary.

PROPOSITION 5.4. *Let $F = \mathbb{Q}(\sqrt[3]{m})$. Then we have,*

(a) $0 \to WD \to WF$ *is* split *exact if m is even.*

(b) *If m is odd, $0 \to WD \to WF$ is* split *exact if and only if $|2 \cdot W_t D| = 2$ (i.e., $s + t = 1$ with the notation of Section 2).*

Proof. Follows immediately from (5.1), (5.3), (2.15), and (2.18).

We shall now compute the order of $2 \cdot W_t D$ in a number of examples, when m is odd. We recall that $|2 \cdot W_t D| = 2^{s+t}$ where $2^s = |U_F^+ / N(K) \cap U_F^+|$ and $2^t = |{}_2H^*(F)/\mathscr{H}|$ (cf. (2.1)). If $|H^*(F)|$ (which is

equal to $|H(F)|$ in this case) is odd, then $t=0$. We compute the integer s for some fields $\mathbb{Q}(\sqrt[3]{m})$.

Our computation is based on the table of positive fundamental units of $F=\mathbb{Q}(\sqrt[3]{m})$ as given in [3, p. 2]. If u is the positive fundamental unit, then $U_F^+ \subset N(K)$ if and only if u is a sum of two squares in F. Since u is a sum of two squares in all the archimedean completions and all the nondyadic, nonarchimedean completions, it follows that $U_F^+ \subset N(K)$ if and only if u is a sum of two squares in the dyadic completions F_1 and F_2. In view of Hensel's lemma (cf. [4, p. 64]), this is equivalent to u being a sum of two squares in $\mathbb{Z}/8\mathbb{Z}$.

EXAMPLE 5.5. Let $F=\mathbb{Q}((\sqrt[3]{3})$. We write $a=\sqrt[3]{3}$. The positive fundamental unit is given by $u=a^2-2$ (cf. [3, p. 2]). We have $u=a^2-2\equiv -1 \bmod 8$ (since a is a unit mod 8, $a^2\equiv 1 \bmod 8$). In view of the above discussions, this implies that $U_F^+/N(K)\cap U_F^+ \simeq \mathbb{Z}/2\mathbb{Z}$. Also $H^*(F)$ is trivial in this case (cf. [1, p. 427]). Thus we have $c=1$, $l=0$, $d=2$, $s=1$, and $t=0$, with the notation of (2.1). Hence $W_t D \simeq \mathbb{Z}/4\mathbb{Z}$ and $WD \simeq \mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$. We also have a split exact sequence

$$0 \to WD \to WF \to \bigsqcup_{\mathfrak{p}\neq 0} W\bar{F}_{\mathfrak{p}} \to 0,$$

since $H(F)$ is trivial.

Table 5.6. is based on computations similar to those above. For the positive fundamental units cf. [3] and for class numbers cf. [1, p. 427].

TABLE 5.6.

Cubic Fields

m	h	$u>0$	Structure of WD	Splitting of $WD \subsetneq WF$?
2	1	$a-1$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	Yes
3	1	a^2-2	$\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	"
5	1	$2a^2-4a+1$	$\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	"
7	3	$-a+2$	$\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	"
11	2	$-2a^2+4a+1$	$\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	"
13	3	$2a^2-3a-4$	$\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$	"
15	2	$12a^2-30a+1$	$\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	"
19	3	$3a-8$	$\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$	No

Note. $F=\mathbb{Q}(a)$, $a\in F$, $a^3=m$, $u=$ positive fundamental unit of F, $h=$ class number of F.

ACKNOWLEDGMENTS

I am indebted and grateful to Dr. R. Parimala, who initiated me to research and whose constant help made this work possible. I am equally grateful to Professor R. Sridharan for his constant encouragement. I thank the referee, whose critical comments led to a better exposition of this paper.

REFERENCES

1. Z. I. BOREVICH AND I. R. SHAFAREVICH, "Number Theory," Academic Press, New York/London, 1966.
2. J. W. S. CASSELS AND A. FRÖHLICH, "Algebraic Number Theory," Academic Press, New York/London, 1967.
3. B. DELAUNAY, Vollstandige Lösung der unbestimmten Gleichung $X^3q + Y^3 = 1$ in ganzen Zahlen, *Math. Z.* **28** (1928), 1–9.
4. M. J. GREENBERG, "Lectures on Forms in Many Variables," Benjamin, New York, 1969.
5. H. HASSE, "Number Theory," Springer-Verlag, Berlin, 1980.
6. I. KAPLANSKY, "Infinite Abelian Groups," Univ. of Michigan Press, Ann Arbor, 1954.
7. T. Y. LAM, "The Algebraic Theory of Quadratic Forms," Benjamin, New York, 1973.
8. J. MILNOR AND D. HUSEMOLLER, "Symmetric Bilinear Forms," Springer-Verlag, Berlin, 1973.
9. W. NARKIEWICZ, "Elementary and Analytic Theory of Algebraic Numbers," Warszawa, 1974.
10. O. T. O'MEARA, "Introduction to Quadratic Forms," Springer-Verlag, Berlin, 1971.
11. W. SCHARLAU, "Quadratic and Hermitian Forms," Springer-Verlag, Berlin, 1985.